FILED
RICHARD W. NAGEL
CLERK OF COURT
4/24/2023
U.S. DISTRICT COURT
SOUTHERN DIST. OHIO
WEST. DIV. DAYTON

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

APPLE IPHONE, IMEI NO. 356825825068711, CURRENTLY LOCATED AT FBI, EV CONTROL ROOM, 2012 RONALD REAGAN DRIVE, CINCINNATI, OHIO

Case No. 3:23-mj-164

APPLICATION FOR A SEARCH WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 371	Conspiracy to commit offense or to defraud United States
18 U.S.C. § 1028	Fraud and related activity in connection with identification documents, authentication features, and information
18 U.S.C. § 1028A	Aggravated identity theft
18 U.S.C. § 1029	Fraud and related activity in connection with access devices

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Matthew Rosenberg
Applicant's signature

SA MATTHEW ROSENBERG, FBI
Printed name and title

Sworn to before me and signed in my presence via telephone.

Date: 4/24/23

City and state: DAYTON, OHIO

Peter B. Silvain, Jr.
United States Magistrate Judge

ATTACHMENT A

1. The property to be searched is an Apple iPhone bearing IMEI number: 356825825068711, previously referenced to as the "Device." The Device is currently stored and maintained in a secure location at the FBI Cincinnati Division - Evidence Control Room - 2012 Ronald Reagan Drive, Cincinnati, Ohio 45236.

2. This requested warrant seeks authority to forensically exam the Device for the purpose of identifying the presence of electronically stored information and data as described in Attachment B.

ATTACHMENT B

1. All records and other electronically stored data and information contained on the Device described in Attachment A that relate to conspiracy in violation of 18 U.S.C. § 371 (conspiracy to commit offense or to defraud United States), 18 U.S.C. § 1028 (fraud and related activity in connection with identification documents, authentication features, and information), 18 U.S.C. § 1028A (aggravated identity theft), and 18 U.S.C. § 1029 (fraud and related activity in connection with access devices).

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF AN APPLE IPHONE, BEARING INTERNATIONAL MOBILE EQUIPMENT IDENTITY (IMEI) NUMBER: 356825825068711, CURRENTLY LOCATED AT THE FBI CINCINNATI DIVISION - EVIDENCE CONTROL ROOM - 2012 RONALD REAGAN DRIVE, CINCINNATI, OH 45236	Case No. 3:23-mj-164

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Matthew Rosenberg, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of certain property—an electronic device—(which is described in Attachment A) which is currently in law enforcement possession, and the extraction from that property of certain electronically stored data/information as described in Attachment B.

2. I, Matthew Rosenberg, am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), currently assigned to the Centerville, Ohio Office which is part of the Cincinnati Division. I have held this position since December 2021. Currently, I am primarily tasked with investigating criminal activity regarding violent crime, white collar fraud, and public corruption. I am a graduate of the FBI's Basic Field Training Course which is located in Quantico, Virginia. As a SA, I am authorized by both Federal law and my Government agency to engage in or supervise the prevention, detection, investigation, or prosecution of violations of Federal

criminal laws. This affidavit is intended to set forth the existence of sufficient probable cause for the requested warrant and does not set forth all of my knowledge about the subject investigation.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

3. The specific property to be searched is an Apple iPhone bearing International Mobile Equipment Identity (IMEI) number: 356825825068711, hereinafter referred to as the "Device." The Device is currently stored in a secure location in the FBI Cincinnati Division's - Evidence Control Room, located at 2012 Ronald Reagan Drive, Cincinnati, Ohio 45236.

4. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying and reviewing certain electronically stored information/data more particularly, described in Attachment B.

PROBABLE CAUSE

5. Your Affiant believes that based upon the following facts and circumstances, there exists probable cause to believe the sought-after evidence (in the form of stored electronic information/data) is stored on the Device that is relevant to an ongoing criminal investigation that is looking into possible violations of Federal law, to wit: 18 U.S.C. §§ 371, 1028, 1028A, and 1029.

Moraine, Ohio – Kroger Incident:

6. On November 11, 2021, a Kroger Grocery Store Loss Prevention Agent, known as WITNESS 1, placed a 911 call to report several individuals were attempting to cash various fraudulent Kroger payroll checks at a Kroger Grocery Store located in Moraine, Ohio which is located in Montgomery County. The Kroger Company, is an American retail company that owns and operates various supermarkets located throughout the United States.

7. In response, at approximately 1:09PM on said date, Moraine Police Department (MPD) Police Officers were dispatched to the subject Kroger Grocery Store located at 2921 West Alex Bell Road Moraine, OH 45459.

8. Upon arriving on scene, MPD Officers observed two possible suspects leaving the target store relevant to WITNESS 1's 911 call. WITNESS 1 provided authorities with a description of two possible get-away vehicles. The vehicles included a white KIA automobile bearing Georgia (GA) registration CRP4812 (VEHICLE 1), and a black Dodge Ram pickup truck bearing GA registration TCP8312 (VEHICLE 2). VEHICLE 2 was later determined, by law enforcement officials, to be a rented vehicle.

9. VEHICLE 2 was observed driving away northbound on State Route 741. The MPD Police Officer followed VEHICLE 2 which thereafter attempted to elude the MPD Police Officer. VEHICLE 2 turned into a parking lot, drove around a building into another parking lot, and then cut through an adjacent field. The MPD Police Officer pursued VEHICLE 2 as it proceeded to drive into an apartment complex parking lot. The driver, and two additional occupants abandoned VEHICLE 2 and fled on foot. Authorities were unable to pursue or locate VEHICLE 1.

10. A foot pursuit of two suspects who exited VEHICLE 2 continued and led across Alex Bell Road. Two suspects were ultimately apprehended by MPD in the parking lot of a business identified as "The Wellington", located at 2656 West Alex Bell Road, Dayton, Ohio 45459. The driver was identified as Gregory PIERRE; the passenger was identified as William Roy WYNN. At the time of their apprehension PIERRE had $1,489.12 in United States (U.S.) currency on his person, while WYNN possessed $5,050.06 in U.S. currency and 5.12 grams of marijuana.

11. MPD Officers secured the abandoned VEHICLE 2. A large blue Nike duffle bag was discovered laying outside adjacent to the truck. Officers checked and cleared this bag for the presence of any possible dangerous ordinance. A computer and printer found inside the bag were seized by MPD.

12. Following their arrest, PIERRE and WYNN were interviewed by MPD. PIERRE admitted to driving VEHICLE 2. Both suspects denied having any knowledge as to anything that may have occurred inside the Kroger store. Both suspects also denied having knowledge about the blue duffle bag.

13. On November 11, 2021, PIERRE and WYNN were arrested on state charges of "Counterfeiting" and "Possession of Criminal Tools" in violation of Ohio Revised Code §§ 2913.30 and 2923.24. On November 22, 2021, both PIERRE and WYNN were released from pre-trial detention pending further investigation.

Investigative Steps Taken by MPD:

14. On or after November 11, 2021, 28 Kroger Payroll Checks were turned into MPD by WITNESS 1. These checks had been turned over to WITNESS 1 by an unidentified individual who found them lying on the ground adjacent to the apartment complex where VEHICLE 2 was ultimately abandoned. These recovered checks consisted of the following:

- 11 checks payable to Shykirra Price, 6374 Oldmadison Pl., Atlanta GA, 30349
- Three checks payable to Ciara Scranton, 1718 Dexter Av., Cincinnati OH, 45206
- Two checks payable to Robert Fite, 225 Wells Street, Elsmere KY, 41018
- Six checks payable to Cameyia R Crawford, 5852 Three Lakes Dr., Atlanta GA, 30349

- Six checks payable to Kevin D Harp, 300 Wendell CT, Jonesboro GA, 30336

These 28 checks totaled approximately $27,834.96 in value. Each appeared to be uncashed fraudulent Kroger payroll checks.

15. On November 12, 2021, MPD Officers executed a state search warrant on VEHICLE 2. MPD located inside the vehicle an additional 28 fraudulent Kroger payroll checks bearing various names totaling approximately $27,781.62 in value.

16. On November 12, 2021, MPD Officers executed an additional state search warrant on the said blue duffle bag. This duffle bag was found to contain a HP laptop bearing serial #CND6511NSY, a HP printer, and a large envelope containing sheets of check printing paper.

17. On November 12, 2021, MPD Officers executed an additional state search warrant on the said HP laptop bearing serial #CND6511NSY. On November 15, 2021, this laptop was turned over to the Warren County Sheriff's Office for forensic review. Several items of evidentiary interest were discovered stored on this laptop, to include: a bank statement, a personal resume for an individual named of PIERRE, and a "Versa Check for QuickBooks" accounting software program. Loaded on this software program was a collection of business checks valued at approximately $591,839.69. This software program also contained a list of payee names and check amounts that corresponded to certain fraudulent Kroger payroll checks that had been passed or had been attempted to be passed at various Kroger's stores located throughout the United States between approximately November 4, 2021, and November 11, 2021.

18. MPD Officers also executed a state search warrant on an iPhone seized from PIERRE's upon his arrest. Data stored in this phone confirmed that PIERRE and WYNN had previously communicated with each other via phone calls and text messages. There were

additionally several screen shots located on PIERRE's iPhone depicting maps, addresses, and directions to various Kroger store locations.

19. As a result of these MPD investigative steps, MPD contacted your Affiant and advised me that PIERRE, WYNN, and other individuals were suspected to be involved in a massive fraud scheme that cashed counterfeit Kroger payroll checks at Kroger Stores located in Bellevue Kentucky (KY), Norwood OH, and at least two locations in Cincinnati, OH, Madeira, OH, Springboro, OH, and Miami Township, OH between November 4th and 11th, 2021. Your Affiant was further advised that Kroger security officials had previously alerted their store employees in Kentucky and Ohio of the existence of this fraud ring.

Identification of Clemons and Williams:

20. As part of MPD's investigation, detectives were able to determine that on or about November 4, 2021, various suspects connected with this fraud scheme had patronized the Hard Rock Casino located in Cincinnati, OH. Specifically, PIERRE and WYNN, along with two other individuals were confirmed to have entered this casino on said date when several counterfeit checks were known to have been cashed by at least two female individuals using the alias names Cameyia CRAWFORD and Shykirra PRICE. Each of the suspected conspirators were required to present photo identification cards upon entering the Casino facility. CRAWFORD was later identified to actually be Jennyfer CLEMONS after referencing her United States passport number 670618004. CLEMONS was later determined to be the registered owner of VEHICLE 1. PRICE was later identified to actually be Chasity WILLIAMS after referencing her Georgia driver's license number 057999473.

21. PIERRE was confirmed to be present at the Hard Rock Casino in Cincinnati, OH on said date after referencing his Georgia driver's license number 052869336. WYNN was

confirmed to be present at the casino on said date after referencing his Georgia driver's license number 051927695.

Harrison County, Mississippi Sheriff's Office Incident:

22. On March 12, 2022, Deputies from the Harrison County, Mississippi Sheriff's Department (HCSD) conducted a traffic stop on an eastbound Interstate Highway 10, a 2017 Dodge Ram 1500 pickup truck bearing GA CLL9342 (VEHICLE 3) near mile marker 33. Subject vehicle was determined to have been following another vehicle too closely. LEO 1 made contact with the driver who was identified to be PIERRE. His passenger was identified to be WYNN. LEO 1 had PIERRE exit his vehicle and join LEO 1 in their patrol car while a computer record check was performed.

23. LEO 1 advised PIERRE that he would only be issuing him a "warning" for the infraction. LEO 1 asked PIERRE where he and WYNN were coming from. PIERRE responded that he had been in Louisiana visiting his daughter. LEO 1 asked what part of Louisiana they visited. PIERRE responded "Lafayette".

24. At that point, LEO 1 returned back to VEHICLE 3 to check the registration and speak with WYNN. LEO 1 then inquired of WYNN as to where they were coming from. WYNN answered "Texas". WYNN further stated they had been to Killeen, Texas visiting "family". LEO 1 returned with WYNN's Georgia ID. LEO 1 conducted a warrant check on WYNN and discovered he had an outstanding Florida warrant. At that point LEO 1 radioed for police backup to respond to the scene. While awaiting the arrival of the backup unit, LEO 1 requested consent to search the vehicle from PIERRE. PIERRE refused this request.

25. Shortly after the arrival of a K9 Unit, the K9 was deployed resulting in a positive "alert" on Vehicle 3. LEO 1 thereafter conducted a probable cause search of the vehicle. LEO 1

observed numerous small pieces of what appeared to be marijuana residue and collected a bigger piece that was consistent in appearance with raw marijuana.

26. LEO 1 also located a green duffel bag sitting on the rear seat on the driver side. Inside the bag was found a Dell laptop computer, a printer, and 300-500 blank checks. LEO 1 found these items to be consistent with counterfeit document-making equipment. LEO 1 thereafter detained PIERRE and placed him into an adjacent patrol car. As part of a subsequent "pat-down" process LEO 1 located the presence of a large amount of cash located in PIERRE's pockets.

27. LEO 1 also located a check stub in the center console of VEHICLE 3. A bank account number and routing number were printed on the check stub. The check stub appeared to be printed on the same type of paper stock located in the green duffel bag. This check stub purportedly was issued by a company named Excel Inc., dba DHL Supply Chain (USA) located at 570 Polaris Parkway Westerville, Ohio 43082. LEO 1 observed an unusual aspect on the check stub, to wit: no federal or state income tax was withheld. LEO 1 further noticed that the pay rate reflected for straight time was $26.50 per hour, while the "overtime pay" was listed as $21.75 per hour. LEO 1 also located another laptop computer inside VEHICLE 3 that apparently belonged to WYNN. This laptop was a HP Laptop Computer, bearing serial number 5CB3523K2Z[1]. LEO 1 patted down PIERRE and found in excess of $7,000 in U.S. currency on his person.

28. LEO 1 seized the said computers, equipment, blank checks, paystub, and WYNN's cell phone. WYNN's cellphone was later identified as an Apple iPhone bearing IMEI number: 356825825068711. This iPhone is hereinafter referred to as the "Device."

---

[1] On January 23, 2023, your affiant telephonically swore out an application for a search warrant of said HP Laptop Computer, bearing serial number 5CB3523K2Z. The search warrant was signed by United States Magistrate Judge Caroline H. Gentry. On January 26, 2023, the FBI executed said search warrant with the assistance of the United States Secret Service. The United States Secret Service analyzed the digital forensic evidence obtained through the search warrant and determined PIERRE and WYNN both utilized the laptop, albeit to a "minimal" extent.

29. LEO 1 ran a criminal history on both subjects and determined both PIERRE and WYNN had previously been arrested together in Ohio for Possessing Counterfeit Equipment. LEO 1 thereafter contacted MPD.

30. LEO 1 ultimately released PIERRE pending further investigation. LEO 1 transported WYNN to the Harrison County Jail due to the outstanding Florida warrant. After arriving at the jail, a strip search was performed on WYNN which resulted in the discovery of an additional approximately $4,000 in cash found hidden under WYNN's scrotum.

31. HCSD officials ultimately contacted MPD officials and briefed them on this incident. Arrangements were made to preserve the said seized evidence. Subsequently the evidence items from the traffic stop were transferred to the FBI. The Device is currently maintained in the lawful care, custody, and control of the FBI.

32. Your Affiant seeks this additional Federal search warrant out of an abundance of caution to ensure that the anticipated search of the Device fully complies with all Fourth Amendment requirements.

33. The Device is currently maintained in secure storage at the FBI Cincinnati Division - Evidence Control Room - 2012 Ronald Reagan Drive, Cincinnati, Ohio 45236. The Device has been stored in a manner such that its contents are, to the maximum extent possible, maintained and preserved in substantially the same state as such when the Device first came into the FBI's possession.

TECHNICAL TERMS

34. Based on your Affiant's prior law enforcement training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication

through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing

computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

35. Based upon my prior law enforcement training and experience, examining stored electronic data on devices of this type can uncover, among other things, evidence that reveals or suggests who previously possessed or used the Device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

36. Based on your Affiant's prior law enforcement knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, electronic data previously viewed via the Internet are typically stored for some period of time on electronic devices. This information can oftentimes be recovered with forensics tools.

37. There is probable cause to believe that data that was once stored on an electronic device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

38. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device

was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

39. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

40. *Manner of execution.* Because this warrant seeks only permission to examine the Device, which is already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, your Affiant submits there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

41. Your Affiant respectfully submits that the aforesaid facts set forth in this affidavit establishes the necessary probable cause to justify the issuance of a search warrant authorizing the examination of the Device as described in Attachment A in order to seek the items described in Attachment B.

Respectfully submitted,

Matthew Rosenberg

Matthew Rosenberg
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on April 24, 2023:

Peter B. Silvain, Jr.
United States Magistrate Judge